2. ARITMÉTICA ENTERA

2.1. El conjunto de los números enteros

Conjuntos de números

- **Números naturales**: $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$
- **Números enteros**: $\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$
- Números racionales: $\mathbb{Q} = \left\{\frac{p}{q} \,:\, p, q \in \mathbb{Z},\, q \neq 0\right\} = \{\text{números con expresión decimal periódica}\}$
- Números reales: $\mathbb{R} = \mathbb{Q} \cup \{\text{números con expresión decimal no periódica}\}$

Operaciones en el conjunto de los números enteros
En $\mathbb{Z}$ se consideran las conocidas operaciones de **suma** y **producto** que verifican las siguientes propiedades:

Conmutativa:	$a + b = b + a$	$ab = ba$
Asociativa:	$a + (b + c) = (a + b) + c$	$a(bc) = (ab)c$
Elemento neutro:	$a + 0 = a$	$1a = a$
Elemento opuesto:	$a + (-a) = 0$	
Distributiva:	$a(b + c) = ab + ac$	
Cancelativa:	$a + c = b + c \;\Rightarrow\; a = b$	$ac = bc$ y $c \neq 0 \;\Rightarrow\; a = b$

Orden natural en $\mathbb{Z}$
Dados dos números enteros a y b, se dice que $a \leq b$, que se lee "a es *menor o igual* que b, si $b - a \geq 0$. Se verifican las siguientes propiedades:

1. Reflexiva: $a \leq a$, para cualquier $a \in \mathbb{Z}$.
2. Antisimétrica: si $a \leq b$ y $b \leq a$, entonces $a = b$.
3. Transitiva: si $a \leq b$ y $b \leq c$, entonces $a \leq c$.
4. Orden total: para cualesquiera $a, b \in \mathbb{Z}$, $a \leq b$ o $b \leq a$.
5. Compatibilidad con la suma: si $a \leq b$ entonces $a + c \leq b + c$ para todo $c \in \mathbb{Z}$.
6. Compatibilidad con el producto: si $a \leq b$ entonces $ac \leq bc$ para todo $c \geq 0$.

Acotación en $\mathbb{Z}$

- Un conjunto $X \subset \mathbb{Z}$ está **acotado inferiormente** si existe un $m \in \mathbb{Z}$, llamado **cota inferior**, tal que $m \leq x$ para todo $x \in X$. La mayor de las cotas inferiores se llama **ínfimo**, y si pertenece al conjunto se llama **mínimo** o **primer elemento**.
- Un conjunto $X \subset \mathbb{Z}$ está **acotado superiormente** si existe un $M \in \mathbb{Z}$, llamado **cota superior**, tal que $x \leq M$ para todo $x \in X$. La menor de las cotas superiores se llama **supremo**, y si pertenece al conjunto se llama **máximo** o **último elemento**.
- Un conjunto se dice que está **acotado** cuando lo está superior e inferiormente.

Axioma de la buena ordenación: Cualquier subconjunto no vacío de $\mathbb{Z}$ acotado inferiormente tiene mínimo.

Y, como consecuencia, también se cumple que:

- Cualquier subconjunto no vacío de $\mathbb{Z}$ acotado superiormente tiene máximo.

- El conjunto de los números naturales y cualquier subconjunto suyo tienen primer elemento.

Relaciones de orden

Se llama **relación de orden** sobre un conjunto A a cualquier relación R entre sus elementos que verifica las siguientes tres propiedades:

1. Reflexiva: aRa, para cualquier $a \in A$.

2. Antisimétrica: si aRb y bRa, entonces $a = b$.

3. Transitiva: si aRb y bRc, entonces aRc.

Cuando además dos elementos cualesquiera siempre están relacionados (para cualesquiera $a, b \in A$, aRb o bRa) se dice que R es un **orden total** o que el conjunto A está **totalmente ordenado** por R. En caso contrario se habla de **orden parcial**.

Ordenes en el conjunto de los números naturales

- Orden natural: $1 < 2 < 3 < 4 < \ldots$.
- Orden de Sarkovski:

$$\begin{array}{ccccccccccc}
 & 3 & \prec & 5 & \prec & 7 & \prec & 9 & \prec & \ldots & \prec \\
\prec & 2\cdot 3 & \prec & 2\cdot 5 & \prec & 2\cdot 7 & \prec & 2\cdot 9 & \prec & \ldots & \prec \\
\prec & 2^2\cdot 3 & \prec & 2^2\cdot 5 & \prec & 2^2\cdot 7 & \prec & 2^2\cdot 9 & \prec & \ldots & \prec \\
\prec & 2^3\cdot 3 & \prec & 2^3\cdot 5 & \prec & 2^3\cdot 7 & \prec & 2^3\cdot 9 & \prec & \ldots & \prec \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\prec & \ldots & \prec & 2^3 & \prec & 2^2 & \prec & 2 & \prec & 1 &
\end{array}$$

- Otro orden total: $1 \lhd 3 \lhd 5 \lhd 7 \lhd \ldots \lhd 2 \lhd 4 \lhd 6 \lhd 8 \lhd \ldots$.
- Un orden parcial: $a \dashv b$ si $a \leq b$ y $b - a$ es par. Un representación de este orden sería:

$$\begin{cases} 1 \dashv 3 \dashv 5 \dashv 7 \dashv \ldots \\ 2 \dashv 4 \dashv 6 \dashv 8 \dashv \ldots \end{cases}$$ y no están relacionados los pares con los impares

Ejercicios

1. Estudia la acotación de los siguientes conjuntos de número enteros:

$$A = \left\{x \in \mathbb{Z} : x^2 < 10\right\} \qquad B = \{x \in \mathbb{Z} : x \text{ es múltiplo de } 3\}$$

Soluciones y/o sugerencia a los ejercicios

1. A está acotado con mínimo -3 y máximo 3. B no está acotado ni inferior ni superiormente.

2. ARITMÉTICA ENTERA

2.2. El método de inducción

Definiciones recursivas
Para definir una función sobre el conjunto de los números naturales se pueden usar dos tipos de expresiones o fórmulas:

- Fórmula **explícita**: cuando basta sustituir n para hallar el valor de la función.
- Fórmula **recursiva**: cuando el valor de la función en n se calcula a partir de los valores que toma en $n-1$, $n-2$, ...

Así, por ejemplo, fórmulas explícita y recursiva para la suma de los n primeros números naturales son las siguientes:

$$\text{Explícita: } S(n) = 1+2+3+\ldots+n = \frac{n(n+1)}{2} \qquad \text{Recursiva: } \begin{cases} S(1) = 1 \\ S(n) = S(n-1) + n\,, \quad n > 1 \end{cases}$$

Definición inductiva de $\mathbb{N}$
Si $S \subset \mathbb{N}$ verifica que:

$$\text{(i) } 1 \in S \qquad \text{(ii) } k \in S \;\Rightarrow\; k+1 \in S$$

entonces $S = \mathbb{N}$.

El principio de inducción
Sea P_n una proposición matemática que puede ser verdadera o falsa para cada número natural n. El **principio de inducción matemática** afirma que si:
(i) P_1 es verdadera.
(ii) P_k verdadera $\Rightarrow$ P_{k+1} verdadera.
Entonces, la P_n es verdadera para cualquier $n \in \mathbb{N}$.

Observación Si en la definición inductiva se cambia la condición "$1 \in S$" por "$n_0 \in S$", $n_0 \in \mathbb{Z}$, entonces $S = \{n_0, n_0+1, \ldots\}$. Como consecuencia, si en el principio de inducción se cambia la condición "P_1 es verdadera" por "P_{n_0} es verdadera" entonces el principio de inducción concluye que P_n es verdadera para cualquier $n \geq n_0$. (¡Ojo!: n_0 puede ser natural o entero.)

El principio de inducción fuerte
Sea P_n una proposición matemática que puede ser verdadera o falsa para cada número natural o entero $n \geq n_0$.
El **principio de inducción fuerte** afirma que si:
(i) P_{n_0} es verdadera.
(ii) P_n verdadera para $n_0 \leq n \leq k$ $\Rightarrow$ P_{k+1} verdadera.
Entonces, la P_n es verdadera para cualquier $n \geq n_0$.

Ejercicios

1. Obtén expresiones recursivas para cada una de las siguientes funciones:
(a) La suma de los n primeros números naturales impares.
(b) La función que proporciona el número total de puntos de corte después de trazar n rectas en el plano con la condición de que cada recta trazada corta a todas las trazadas con anterioridad.
(c) El factorial del número n.

2. Demuestra, usando el principio de inducción matemática, que para cualquier número natural $n \in \mathbb{N}$ se

cumple cada una de las siguientes propiedades:

(a) $1^2 + 2^2 + 3^2 + \ldots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$

(b) $1^3 + 2^3 + 3^3 + \ldots + n^3 = \left(\dfrac{n(n+1)}{2}\right)^2$

(c) $1^4 + 2^4 + 3^4 + \ldots + n^4 = \dfrac{n(n+1)(6n^3+9n^2+n-1)}{30}$

(d) $\dfrac{1}{1\cdot 2} + \dfrac{1}{2\cdot 3} + \dfrac{1}{3\cdot 4} + \ldots + \dfrac{1}{n(n+1)} = \dfrac{n}{n+1}$

(e) $(1+a)^n \geq 1 + an$, siendo $a > 0$

(f) $n^3 + (n+1)^3 + (n+2)^3$ es divisible por 9

(g) $n^3 - n$ es divisible por 6

(h) $2^n < n!$, si $n \geq 4$

(i) $7^n - 1$ es divisible por 6

(j) $2^{2n} + 15n - 1$ es múltiplo de 9

(k) $2^{2n} > n^2$

(l) $3 \cdot 5^{2n+1} + 2^{3n+1}$ es múltiplo de 17

Soluciones y/o sugerencia a los ejercicios

1. (a) $\begin{cases} S(n) = S(n-1) + (2n-1)\,,\ n > 1 \\ S(1) = 1 \end{cases}$. **(b)** $\begin{cases} C(n) = C(n-1) + (n-1)\,,\ n > 1 \\ C(1) = 0 \end{cases}$.

(c) $\begin{cases} F(n) = nF(n-1)\,,\ n > 1 \\ F(1) = 1 \end{cases}$.

(2) En cada caso, se verifica que la propiedad es cierta para $n = 1$ (en (h) para $n = 4$) y después, suponiendo que la igualdad es cierta para $n = k - 1$ se demuestra que es cierta para $n = k$.

2. ARITMÉTICA ENTERA

2.3. Sistemas de numeración

Teorema de la división entera
Si $a \in \mathbb{Z}$ y $b \in \mathbb{N}$, entonces existe un único par de enteros $q, r \in \mathbb{Z}$ tales que:

$$a = bq + r \qquad \text{con} \qquad 0 \leq r < b$$

Demostración: Se supone, en primer lugar, que $a \geq 0$.
Existencia: Se considera el conjunto $X = \{n \in \mathbb{Z} : n \geq 0 \text{ y } nb \leq a\}$. Este conjunto es no vacío, ya que al menos $0 \in X$, y está acotado superiormente, luego admite máximo $q \in X$ que verifica:

$$\begin{cases} qb \leq a \implies a - qb \geq 0 \\ a - qb < b \text{ , pues si } a - qb \geq b \text{ entonces } (q+1)b \leq a \text{ y } q \text{ no sería supremo} \end{cases} \implies a - qb = r \text{ con } 0 \leq r < b$$

Unicidad: Si $a = q_1 b + r_1$ y $a = q_2 b + r_2$, restando ambas expresiones:

$$(q_1 - q_2)b = r_2 - r_1 \implies |q_1 - q_2|\, b = |r_2 - r_1| < b \implies q_1 = q_2 \implies r_1 = r_2$$

Si $a < 0$, entonces $-a > 0$ y se aplica lo anterior: $-a = qb + r$ con $0 \leq r < b$. En el caso de que $r = 0$, $a = -qb + 0 = q'b + 0$, y si $r > 0$:

$$a = -qb - r = -qb - b + b - r = -(q+1)b + (b - r) = q'b + r' \text{ con } 0 < r' = b - r < b$$

Ejemplo: Si $a = 23$ y $b = 7$, $23 = 3 \cdot 7 + 2$, es decir, $q = 3$ y $b = 2$.
Si $a = -23$ y $b = 7$, $23 = 3 \cdot 7 + 2$, y entonces

$$-23 = -3 \cdot 7 - 2 = -3 \cdot 7 - 7 + 7 - 2 = -4 \cdot 7 + 5 \implies q = -4 \text{ y } r = 5$$

Sistema de numeración en base t
Si $t \geq 2$ es un número natural, aplicando el teorema de la división entera, cualquier número natural $x \in \mathbb{N}$ se puede expresar de modo único en la forma:

$$x = r_n t^n + r_{n-1} t^{n-1} + \ldots + r_2 t^2 + r_1 t^1 + r_0 \qquad \text{donde } 0 \leq r_i < t \text{ y } r_n \neq 0$$

y se indica:

$$x = (r_n r_{n-1} \ldots r_2 r_1 r_0)_t$$

que se llama expresión de x en el **sistema de numeración en base** t. Cada $r_i \in \{0, 1, 2, \ldots, t-1\}$ se llama **dígito** en base t.

Ejemplos de bases

- **Base decimal o usual:** $t = 10$, Dígitos= $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
  $204 = 2 \cdot 10^2 + 0 \cdot 10 + 4 = 204_{10}$.
- **Base binaria:** $t = 2$, Dígitos= $\{0, 1\}$.
  $204 = 1 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 0 = 11001100_2$.
- **Base ternaria:** $t = 3$, Dígitos= $\{0, 1, 2\}$.
  $204 = 2 \cdot 3^4 + 1 \cdot 3^3 + 1 \cdot 3^2 + 2 \cdot 3 + 0 = 21120_3$.
- **Base octal:** $t = 8$, Dígitos= $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$.
  $204 = 3 \cdot 8^2 + 1 \cdot 8 + 4 = 314_8$.
- **Base hexadecimal:** $t = 16$, Dígitos= $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9,$ A,B,C,D,E,F$\}$.
  $204 = 12 \cdot 16 + 12 = \text{CC}_{16}$.

2. ARITMÉTICA ENTERA

2.4. Divisibilidad. Algoritmo de Euclides.

Definición de divisibilidad
Dados dos números enteros, $a, b \in \mathbb{Z}$ con $a \neq 0$, se dice que a **divide** a b, y se escribe $a \,|\, b$, si existe un número entero $c \in \mathbb{Z}$ tal que $b = ac$. También a divide a b, también se dice que a es un **divisor** de b o que b es **múltiplo** de a.
El conjunto de divisores positivos de un número positivo b se representa por D_b, y este conjunto siempre contiene a 1 y b.
Un número natural mayor que 1 se llama **primo** si sus únicos divisores son él mismo y la unidad. En caso contrario se llama **compuesto**.

Propiedades de la divisibilidad
Para cualesquiera enteros con el requerimiento, en su caso, de que el divisor sea distinto de cero, se cumplen las siguientes propiedades:

1. $a \,|\, 0\,, \quad \pm 1 \,|\, a\,, \quad \pm a \,|\, a.$ **2.** $a \,|\, b$ y $a \,|\, c \implies a \,|\, (\alpha b + \beta c).$ **3.** $a \,|\, b$ y $b \,|\, a \implies a = \pm b.$

Máximo común divisor
Se llama **máximo común divisor** de dos números enteros no nulos a y b al mayor de sus divisores comunes, y se representa por $\mathrm{mcd}(a, b)$.
Cuando el máximo común divisor de dos números a y b es 1, se dice que dichos números son **primos entre sí**.

Propiedades del máximo común divisor

1. Si $d = \mathrm{mcd}(a, b)$, entonces: $d \,|\, a$ y $d \,|\, b$.

2. Si $c \,|\, a$ y $c \,|\, b$, entonces: $c \,|\, \mathrm{mcd}(a, b)$.

3. Si $a \,|\, bc$ y $\mathrm{mcd}(a, b) = 1$, entonces: $a \,|\, c$.

4. Si $d = \mathrm{mcd}(a, b)$, entonces: $\mathrm{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

5. La reducción de fracciones a forma irreducible es única.

Algoritmo de Euclides para el cálculo del máximo común divisor
Si r es el resto de la división entera entre dos números a y b, entonces $a = bq + r$, de donde se deduce inmediatamente que cualquier divisor de a y b lo es de r y cualquier divisor de b y r lo es de a. En consecuencia: $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r)$.
Mediante sucesivas divisiones enteras se obtiene el algoritmo:

$$\left\{\begin{array}{lcll} a = bq_1 + r_1 & \Longrightarrow & \mathrm{mcd}(a,b) = \mathrm{mcd}(b,r_1) & \\ b = r_1 q_2 + r_2 & \Longrightarrow & \mathrm{mcd}(b,r_1) = \mathrm{mcd}(r_1,r_2) & \\ r_1 = r_2 q_3 + r_3 & \Longrightarrow & \mathrm{mcd}(r_1,r_2) = \mathrm{mcd}(r_2,r_3) & \Longrightarrow \ \mathrm{mcd}(a,b) = r_k \ \text{(último resto no nulo)} \\ \cdots & \cdots & \cdots & \\ r_{k-1} = r_k q_{k+1} + 0 & \Longrightarrow & \mathrm{mcd}(r_{k-1}, r_k) = \mathrm{mcd}(r_k, 0) = r_k & \end{array}\right.$$

Este algoritmo admite el siguiente esquema gráfico:

	q_1	q_2	q_3	$\cdots$	$\cdots$	q_k	q_{k+1}
a	b	r_1	r_2	$\cdots$	$\cdots$	r_{k-1}	$\mathbf{r_k}$
r_1	r_2	r_3	$\cdots$	$\cdots$	r_k	$\mathbf{0}$	

$\Longrightarrow \quad \mathrm{mcd}(\mathbf{a}, \mathbf{b}) = \mathbf{r_k}$

Complejidad del algoritmo de Euclides
Se entiende por complejidad de un algoritmo al número de pasos que hay que realizar hasta que finalize, lo que

depende de los datos iniciales. En cada paso de este algoritmo, el producto de los dos números a los que hallar el máximo común divisor baja al menor a la mitad, ya que:

$$a = bq + r \geq b + r > 2r \implies ab > 2br \implies br < \frac{ab}{2}$$

Después de k pasos se trabaja con dos números cuyo producto es como máximo $\frac{ab}{2^k}$, que tendrá que ser mayor o igual que 1, y entonces:

$$\frac{ab}{2^k} \geq 1 \implies 2^k \leq ab \implies k \leq \log_2(ab) = \log_2 a + \log_2 b$$

Ejercicios

1. Demuestra que para todo $n \geq 1$, 6 divide a $n^3 + 3n^2 + 2n$.

2. Encuentra el conjunto de divisores positivos del número 20. ¿Cuántos son? ¿Cuál es su suma?

3. Usa el algoritmo de Euclides para encontrar el máximo común divisor de los siguientes números: **(a)** 18 y 122; **(b)** 1312 y 800; **(c)** 322 y 406; **(d)** 247 y 9981; **(e)** 10223 y 33341.

Soluciones y/o sugerencia a los ejercicios

1. Se deduce de la descomposición factorial de $n^3 + 3n^2 + 2n$.
2. $D_{20} = \{1, 2, 4, 5, 10, 20\}$. Son 6 y su suma es 42.
3. **(a)** 2; **(b)** 32; **(c)** 14; **(d)** 1; **(e)** 1.

Ejercicios

1. Escribe el número 1465 en bases 2, 5, 7, 8 y 16.
2. Escribe en base decimal los números: 101001001_2, 12101_3, 342104_5 y $2AE0B_{16}$.
3. Resuelve la ecuación: $132_x = 330_5$.
4. Calcula la siguiente suma en base 5: $132_5 + 310_5 + 12_5$.

Soluciones y/o sugerencia a los ejercicios

1. $1465 = 10110111001_2 = 21330_5 = 4162_7 = 2671_8 = 5B9_{16}$.
2. $101001001_2 = 329$, $12101_3 = 145$, $342104_5 = 12154$ y $2AE0B_{16} = 175627$.
3. $x = 8$.
4. 1004_5.

2. ARITMÉTICA ENTERA

2.5. Ecuaciones diofánticas lineales

Definición
Se llama **ecuación diofántica lineal** a cualquier ecuación de la forma $ax+by=c$ donde a, b y c son números enteros y de las que sólo interesan soluciones enteras.

Teorema de Bezout
Dados dos números enteros a y b, $\text{mcd}(a,b)=1$ si y sólo si existen números enteros m y n tales que $ma+nb=1$. Los números m y n no son únicos, como se justifica con el siguiente ejemplo:

$$1=\mathbf{4}\cdot 2+(\mathbf{-1})\cdot 7=(\mathbf{-3})\cdot 2+\mathbf{1}\cdot 7=(\mathbf{-10})\cdot 2+\mathbf{3}\cdot 7=\mathbf{25}\cdot 2+(\mathbf{-7})\cdot 7=\dots$$

Si $\text{mcd}(a,b)=d>1$, también existen números enteros m y n tales que $ma+nb=d$, como se justifica así:

$$\text{mcd}(a,b)=d>1 \implies \text{mcd}\left(\frac{a}{d},\frac{b}{d}\right)=1 \implies \exists m,n\in\mathbb{Z}\,:\, m\frac{a}{d}+n\frac{b}{d}=1 \implies ma+nb=d$$

Algoritmo para encontrar los coeficientes del teorema de Bezout
Para encontrar los coeficientes, cuya existencia asegura el teorema de Bezout, se puede usar un algoritmo que se deriva del algoritmo de Euclides, y que se ilustra a continuación con un ejemplo. Si $a=122$ y $b=18$, entonces $d=\text{mcd}(a,b)=2$ y los coeficientes se obtienen así:

	6	1	3	2
122	18	14	4	**2**
14	4	2	**0**	

$\iff$

$$\begin{aligned}122&=6\cdot 18+14\\18&=1\cdot 14+4\\14&=3\cdot\ \ 4+\mathbf{2}\\4&=2\cdot\ \ 2+\mathbf{0}\end{aligned}$$

$\implies$

$$\begin{aligned}2&=14-3\cdot 4=\\&=14-3(18-1\cdot 14)=4\cdot 14-3\cdot 18=\\&=4(122-6\cdot 18)-3\cdot 18=\mathbf{4}\cdot 122+(\mathbf{-27})\cdot 18\end{aligned}$$

Resolución de las ecuaciones diofánticas lineales
La ecuación diofántica lineal $ax+by=c$, con $a,b,c\in\mathbb{Z}-\{0\}$, tiene solución si y sólo si $\text{mcd}(a,b)\,|\,c$, en cuyo caso las soluciones son:

$$\begin{cases}x=x_0+\frac{bt}{\text{mcd}(a,b)}\\ y=y_0-\frac{at}{\text{mcd}(a,b)}\end{cases}$$ para cualquier $t\in\mathbb{Z}$, siendo (x_0,y_0) una solución particular de $ax+by=c$.

Algoritmo para la resolución de ecuaciones diofánticas lineales
Para resolver la ecuación diofántica lineal $ax+by=c$, que debe verificar que $\text{mcd}(a,b)=d\,|\,c$, se procede así:

1. Se aplica el teorema de Bezout a los números a y b para encontrar m y n verificando que $ma+nb=d$.
2. Multiplicando por $\alpha=c/d$, se obtiene $\alpha ma+\alpha nb=\alpha d$, es decir, $a\alpha m+b\alpha n=c$, de donde se deduce que $x_0=\alpha m$ e $y_0=\alpha n$ es una solución particular.
3. Todas las soluciones de la ecuación son:

$$\begin{cases}x=x_0+\frac{bt}{d}\\ y=y_0-\frac{at}{d}\end{cases},\ t\in\mathbb{Z} \qquad \text{o también:} \qquad \begin{cases}x=\frac{mc+bt}{d}\\ y=\frac{nc-at}{d}\end{cases},\ t\in\mathbb{Z}$$

Ejercicios

1. Estudia la existencia de soluciones y resuelve las siguientes ecuaciones diofánticas lineales:

(a) $28x+7y=10$ **(c)** $165x+48y=-6$ **(e)** $66x+550y=88$ **(g)** $10x-15y=c\,,\ 1\le c\le 12$
(b) $35x-20y=5$ **(d)** $28x+36y=44$ **(f)** $966x+686y=70$ **(h)** $84x+990y=c\,,\ 10<c<20$

2. Se dispone de dos recipientes con capacidad de 7 y 9 litros, respectivamente, un gran cubo con un desagüe y un suministro ilimitado de agua. ¿Es posible conseguir exactamente un litro de agua? ¿Y si no se dispone del cubo?

3. Un turista europeo y otro americano se encuentran en Suecia donde el primero de ellos contrae con el segundo una deuda de 1000 coronas. Si cada uno de ellos dispone de la moneda de su país, sin fracciones, y teniendo en cuenta que un euro equivale a 18 coronas y un dólar a 13 coronas, ¿cómo pueden saldar su deuda?

4. Un agente tiene invertido dinero en acciones de Azucarera y Repsol, cada una de las cuales se cotiza a 89 y 614 euros, respectivamente. Necesita hacer una transacción para disponer exactamente de 1000 euros en efectivo. ¿Cómo puede hacerlo?

Soluciones y/o sugerencia a los ejercicios

1. **(a)** Sin solución. **(b)** $\begin{cases} x = -1 - 20t \\ y = -2 - 35t \end{cases}$ $t \in \mathbb{Z}$. **(c)** $\begin{cases} x = -14 + 16t \\ y = 48 - 55t \end{cases}$ $t \in \mathbb{Z}$. **(d)** $\begin{cases} x = 44 + 9t \\ y = -33 - 7t \end{cases}$ $t \in \mathbb{Z}$.
(e) $\begin{cases} x = -32 + 25t \\ y = 4 - 3t \end{cases}$ $t \in \mathbb{Z}$. **(f)** $\begin{cases} x = -110 + 49t \\ y = 155 - 69t \end{cases}$ $t \in \mathbb{Z}$. **(g)** Si $c = 5$: $\begin{cases} x = -1 + 3t \\ y = -1 + 2t \end{cases}$ $t \in \mathbb{Z}$;
si $c = 10$: $\begin{cases} x = -2 + 3t \\ y = -2 + 2t \end{cases}$ $t \in \mathbb{Z}$; y si $c \neq 5, 10$ no hay solución. **(h)** Si $c = 12$: $\begin{cases} x = 118 + 165t \\ y = -10 - 14t \end{cases}$ $t \in \mathbb{Z}$;
si $c = 18$: $\begin{cases} x = 177 + 165t \\ y = -15 - 14t \end{cases}$ $t \in \mathbb{Z}$; y si $c \neq 12, 18$ no hay solución.

2. Si, echando cuatro veces el recipiente de 7 litros y sacando tres veces el de 9 litros. También.

3. El europeo le paga 57 euros y el americano le devuelve 2 dólares.

4. Vende 69000 acciones de Azucarera y compra 10000 acciones de Repsol.

2. ARITMÉTICA ENTERA

2.6. Números primos

Definición
Un número natural $p > 1$ se llama **primo** si sus únicos divisores positivos son 1 y p. En caso contrario, se llama **compuesto**.
Los primeros números primos son: 2, 3, 5, 7, 11, 13, 17, 19, ...

Teorema fundamental de la aritmética
Todo número natural $n > 1$ se puede expresar de modo único (salvo orden) como producto de números primos:

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$$

donde los números a_i son naturales y los p_i números primos distintos. A esta expresión se le llama **factorización prima** o **descomposición en factores primos** del número n.

Propiedades

1. Un número primo p divide a n si y sólo si p es un factor de la descomposición factorial de n.
2. Si p es primo y $p \,|\, ab$, entonces $p \,|\, a$ o $p \,|\, b$.
3. Si p es primo y $p \,|\, a_1 a_2 \ldots a_k$, entonces $p \,|\, a_i$ para algún i, $1 \leq i \leq k$.
4. Existen infinitos números primos.
5. Un número natural $n > 1$ es compuesto si y sólo si es divisible por algún primo $p \leq \sqrt{n}$.

Criba de Eratóstenes
Es un método sistemático para construir la lista de los números primos hasta cierto número natural N. Se procede así:

- Se escribe una lista ordenada con los números naturales del 2 al N.
- Se deja el número 2 y se tachan todos sus múltiplos: 4, 6, 8, ...
- A partir del 2 el primer número no tachado es 3, que se deja y se tachan todos sus múltiplos: 6, 9, 12, ... (algunos ya estaban tachados).
- A partir del 3 el primer número no tachado es 5, que se deja y se tachan todos sus múltiplos: 10, 15, 20, ... (algunos ya estaban tachados).
- Y así sucesivamente, se continúa mientras que el siguiente número no tachado sea menor o igual que $\sqrt{N}$.

Después del proceso anterior, los números no tachados son los números primos menores o iguales que N.
La criba de Eratóstenes no es útil para decidir si un número grande (de los utilizados en criptografía) es primo. Así, por ejemplo, para saber si es primo un número de 100 cifras, $N \simeq 10^{100}$, la criba de Eratóstenes necesitaría chequear con alrededor de $8 \cdot 10^{47}$ números primos, y para realizar esta tarea las más avanzadas computadoras actuales necesitarían alrededor de 15.000 millones de años (un tiempo mayor que el estimado para la edad del universo).

Resultados y conjeturas sobre números primos

- Todo número natural par es suma de dos número primos (**conjetura de Goldbach**).
- Si $\text{mcd}(a, b) = 1$, existen infinitos números primos de la forma $aq + b$ (**Dirichlet, 1837**).
- El intervalo entre números primos consecutivos puede ser infinitamente grande, como se deduce de que para cualquier n los siguientes $n - 1$ números son compuestos y consecutivos:

$$n! + 2\,, \;\; n! + 3\,, \;\; n! + 4\,, \;\ldots\,, \;\; n! + n\,,$$

- **Primos de Fermat:** son los números de la forma $F_n = 2^{2^n} + 1$, sobre los que conjeturó que todos eran primos. Efectivamente, los primeros sí lo son: $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, ...
  Sin embargo la conjetura no es cierta, como comprobó Euler con el quinto número que es compuesto: $F_5 = 4294967297 = 641 \cdot 6700417$.

- **Números (primos) de Mersenne:** son los números de la forma $M_p = 2^p - 1$ con p primo. Los primeros números de Mersenne son primos: $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$, ...
  Sin embargo, no todos son primos: $M_{11} = 2047 = 23 \cdot 89$ es compuesto.

- Los primos conocidos con un gran número de cifras son siempre primos de Mersenne. A la búsqueda de grandes números primos se dedica el proyecto GIMPS, que en agosto de 2008 encontró el número primo:

$$n = 2^{43112609} - 1 \qquad (\sim 13 \text{ millones de dígitos})$$

- ¿Cuántos números primos hay?: Se sabe que hay infinitos, pero ¿cuántos?

$$\text{Para cada } n, \text{ entre los } n \text{ primeros números naturales hay } \pi(n) \simeq \frac{n}{\ln n} \text{ números primos}$$

Ejercicios

1. Factoriza el número $n = 8872$.

2. Halla todos los múltiplos de 28 cuyas dos últimas cifras sean 16.

3. Demuestra que si $p \neq 2, 5$ es primo, entonces: $10 \,|\, (p^2 - 1)$ ó $10 \,|\, (p^2 + 1)$.

Soluciones y/o sugerencia a los ejercicios
1. $8872 = 2^3 \cdot 1109$.
2. $700t - 784$, $t \geq 2$.
3. Analiza los casos posibles en función de la terminación de p (1, 3, 7 o 9).

2. ARITMÉTICA ENTERA

2.7. Polinomios

Divisibilidad de polinomios
Dados dos polinomio $P(x)$ y $Q(x)$ (con coeficientes enteros), se dice que $Q(x)$ **divide** a $P(x)$, y se indica $Q(x) \,|\, P(x)$, si $P(x) = Q(x)R(x)$, donde $R(x)$ es un polinomio no constante con coeficientes enteros.

Máximo común divisor
Se llama **máximo común divisor** de dos polinomios no constantes $P(x)$ y $Q(x)$ a su divisor común de mayor grado, y se representa por $\text{mcd}(P, Q)$.
Para hallar el máximo común divisor de dos polinomios se puede utilizar el algoritmo de Euclides, como se muestra en el siguiente ejemplo.

Ejemplo
Para hallar el máximo común divisor de los polinomios $P(x) = 2x^4 - x^3 - 5x^2 + 3x$ y $Q(x) = 2x^3 - x^2 - x - 3$ se aplica el algoritmo de Euclides:

	x	$x+1$	x
$2x^4 - x^3 - 5x^2 + 3x$	$2x^3 - x^2 - x - 3$	$2x^2 - 3x$	$\mathbf{2x - 3}$
$-4x^2 + 6x$	$2x - 3$	$\mathbf{0}$	

$\Longrightarrow \quad \text{mcd}(P, Q) = 2x - 3$

Al pasar el primer resto $(-4x^2 + 6x)$ como cociente $(2x^2 - 3x)$ se ha dividido por -2, lo que no afecta el resultado final y evita coeficientes fraccionarios. Asimismo, cuando hay fracciones en algún polinomio, se puede multiplicar por el mínimo común múltiplo de los denominadores.

Factorización de polinomios
Un polinomio $P(x)$ (con coeficientes enteros) es **reducible** si $P(x) = Q(x)R(x)$, donde $Q(x)$ y $R(x)$ son polinomios no constantes con coeficientes enteros. En caso contrario, se dice que $P(x)$ es **irreducible**.
Se llama **factorización** de un polinomio al proceso de descomposición del polinomio en producto de factores irreducibles.

Criterio de Eisenstein
Sea $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$ un polinomio de grado n con coeficientes enteros. Si existe un número primo p que divide a a_0, a_1, $\ldots$, a_{n-1} pero no divide a a_n y p^2 tampoco divide a a_0, entonces $P(x)$ es irreducible.
Así, por ejemplo, para decidir si el polinomio $P(x) = x^3 - 2x^2 + 4x - 6$ es irreducible hay que comprobar si alguno de los número primos que dividen al termino independiente (2 ó 3) verifica el criterio de Eisenstein. Puesto que $p = 2$ lo verifica, el polinomio $P(x) = x^3 - 2x^2 + 4x - 6$ es irreducible.

Ejercicios

1. Halla el máximo común divisor de los siguientes pares de polinomios:

(a) $\begin{cases} P(x) = x^4 - x^3 + 4x^2 - x + 3 \\ Q(x) = x^5 + 2x^3 + 3x^2 \end{cases}$ **(b)** $\begin{cases} P(x) = 2x^4 - 3x^3 - 3x^2 + 2x \\ Q(x) = x^4 - x^3 - 7x^2 + x + 6 \end{cases}$

2. Aplica el criterio de Eisenstein para probar que el polinomio $P(x) = x^3 - 4x + 2$ es irreducible.

3. ¿Son irreducibles los polinomio $P(x) = x^2 + x \pm 1$? ¿Se puede aplicar el criterio de Eisenstein?

Soluciones y/o sugerencia a los ejercicios
1. **(a)** $x^2 - x + 3$; **(b)** $x + 1$.
2. Se cumple para $p = 2$.
3. No se puede aplicar el criterio de Eisenstein. $x^2 + x + 1$ es irreducible, y $x^2 + x - 1$ no lo es.